



**Symantec**



**Norton Personal  
Firewall 2003**

*auch enthalten in  
Symantec Internet Security*

*j.meissburger@fz-juelich.de*



***ein Webfilter und  
persönliches Firewall für Internet-PCs***

ZAM technische Kurzinformation  
[ZAM-TKI-0376 \(Norton Personal Firewall 2002\)](#)

und interner Bericht  
[ZAM-IB-9916](#)



<http://www.fz-juelich.de/zam/net/security>

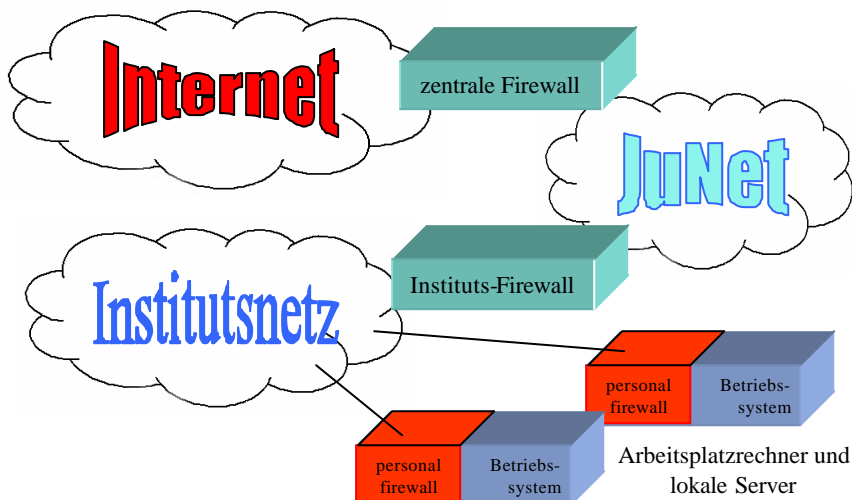


## Funktionen eines persönlichen IP-Firewalls

- Filtern und Steuern des IP- und ICMP-Verkehrs nach Adressen und Domänen
- Filtern und Steuern der Anwendungen nach IP-Ports (Dienste) und Anwendungen
- Unterscheidung von einlaufendem („inbound“) und auslaufendem („outbound“) Datenverkehr
- Erkennen besonderer, potentiell gefährlicher Dateninhalte (Web)
- Schutz vor Weitergabe persönlicher Daten
- Logging von Ereignissen und Statistik
- Nicht:
  - Verbergen oder Umschreiben von Netzadressen (address translation)
  - Logische Verknüpfung von durch Filterregeln definierten Ereignissen



## Die Anordnung von Firewalls im Firmennetz





## Firewalls

- Ein Schutzwall für IP-Kommunikation zwischen
  - Firmen-Firewall: Zwischen dem weltweiten Internet und dem lokalen Firmennetz am zentralen Zugangspunkt zum Internet (Internet ↔ JuNet)
  - Abteilungs-Firewall: Zwischen dem firmenweiten Netz und dem lokalen Netz, in dem sich der eigene Rechner befindet (JuNet ↔ zamnet)
  - Persönliche Firewall: Zwischen dem lokalen Hausnetz und dem eigenen Rechner (zamnet ↔ ZAM-Rechner)
- Eine persönliche Firewall schützt auch
  - gegen ungewollte Kommunikation im eigenen Hausnetz, beispielsweise durch falsch konfigurierte Rechner oder durch Neugier von Kollegen
  - vor allem gegen Angriffe, die von Rechnern im eigenen Netz ausgehen, die bereits von Hackern „übernommen“ worden sind
  - häufig auch gegen Gefährdung durch unvorsichtige Navigation im Web (Skripting, aktive Inhalte)



## persönliche (Desktop) Firewalls

- Microsoft Internet Verbindungsfirewall (Bestandteil von Windows XP)
- Tiny Personal Firewall
  - <http://www.tinysoftware.com>
- ZoneAlarm
  - <http://www.zonealarm.com>
- Norton Personal Firewall 2002/3
  - [http://www.fz-juelich.de/zam/docs/tki/tki\\_html/t0376/t0376.html](http://www.fz-juelich.de/zam/docs/tki/tki_html/t0376/t0376.html)
- AtGuard (lizenziert für FZJ, verfügbar auf <\\zelcds\atguard>, verwendbar bis Windows-2000 )
  - [http://www.fz-juelich.de/zam/docs/tki/tki\\_html/t0349/t0349.html](http://www.fz-juelich.de/zam/docs/tki/tki_html/t0349/t0349.html)
  - <http://www.fz-juelich.de/zam/docs/printable/ib/ib-99/ib-9916.pdf>



# *Symantec Norton Personal Firewall 2003*

**ZAM-TKI-0376**

**Das AtGuard-Nachfolgeprodukt**

**für**

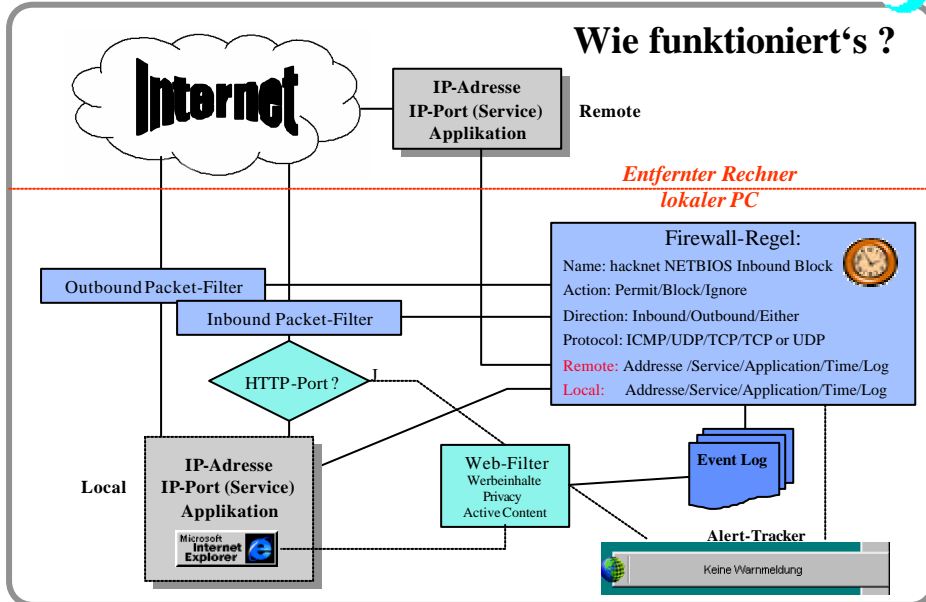
**Windows 95b bis Windows -XP**

**mit halbautomatischer Selbstkonfiguration**



## **Was ist Symantec Norton Personal Firewall ?**

- Ein Monitor- und Statistikwerkzeug für ein- und ausgehende IP-Verbindungen (Dashboard, Regel- und Filter-Assistent, Eventlog).
- Ein regelbasiertes Firewall für ICMP- und IP-Pakete. Berücksichtigt werden:
  - Quell- und Zieladresse
  - Art des Dienstes (Quell- und Ziel-IP-Port)
  - Die dienstvermittelnde Applikation
  - Wochentag und Uhrzeit
- Ein Webfilter für:
  - Werbeinhalte (Inbound)
  - Persönliche Benutzerinformationen (Outbound)
  - Aktive, potentiell gefährliche Web-Inhalte (Inbound Scripting, ActiveX, Java)
- Ein Alarmierungswerkzeug für unerwünschte Verbindungsversuche



## Installation von Norton Personal Firewall 2002/3

- Windows-übliche Installation mit „Weiter.....“

The installation process is shown through three screenshots:

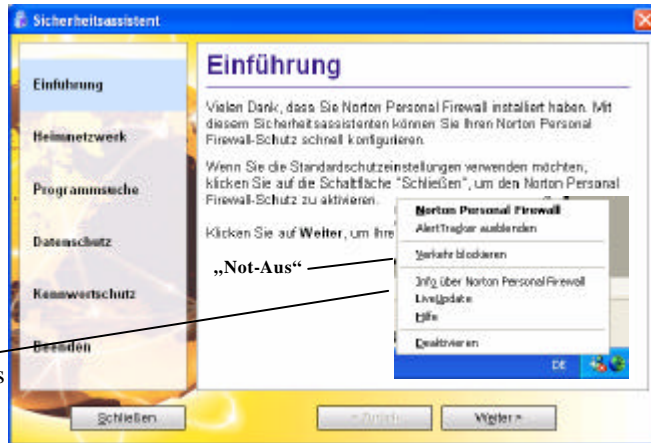
- Willkommen von Norton:** The initial welcome screen of the Norton Personal Firewall 2002/3 installation.
- Registrieren Sie Norton Personal Firewall:** The registration screen where the user provides their name and country (Germany).
- Danke, dass Sie die Registrierung durchgeführt haben:** A message of thanks and confirmation that the registration was successful.

- Registrierung für Einzelplatzsysteme (wichtig für Support)



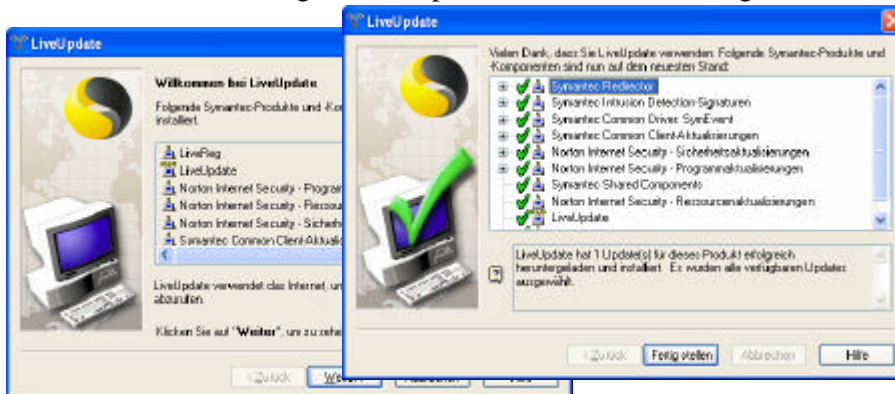
## Konfiguration mit dem Sicherheitsassistenten

- Vereinfachte (?) Einstellung von Firewall (IP-Sicherheit) und Webfiltern (Datenschutz) durch den Sicherheitsassistenten
- Sicherheitsassistent startet automatisch
- Mit „Schließen“ wird das Firewall mit den Standard-einstellungen aktiviert
- Konfiguration kann jederzeit durch Doppelklick auf das Symbol verändert werden



## Live-Update nach Installation

- Installiert aktuelle Programmkomponenten und Firewall-Regeln

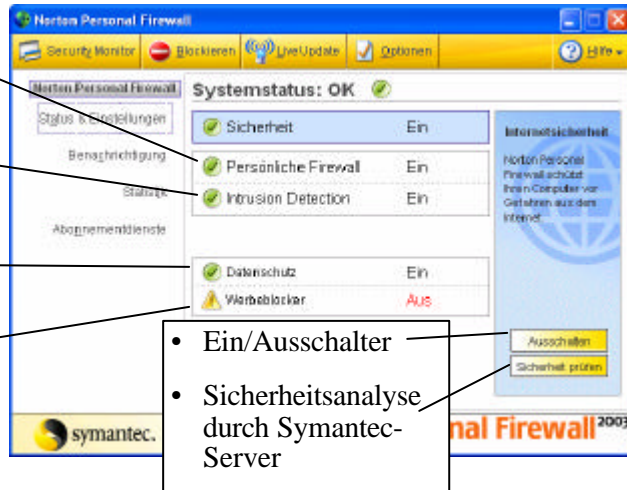


- Kann jederzeit mit „Norton Personal Firewall – Live Update“ erneut ausgeführt werden!



## Norton Personal Firewall (Konsole) Status und Einstellungen

- IP-Firewall-Regelwerk
- Automatischer Schutz vor Angriffen
- Schutz persönlicher Daten
- Werbebanner und PopUp-Windows

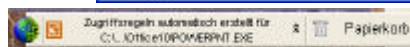


- Ein/Ausschalter
- Sicherheitsanalyse durch Symantec-Server



## Benachrichtigung

- Legt fest, welche Warnmeldungen an den Benutzer gesandt werden
- Aktuelle Meldungen werden auch im Alert-Tracker auf dem Desktop angezeigt:

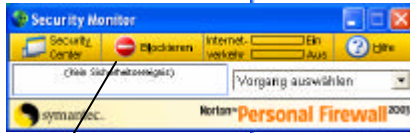




## Statistik

- Überblick über Angriffsversuche und Inhaltsblockierungen

- Eine Mini-Statistik wird auch im Security-Monitor angezeigt:



- „Not-Aus“ stoppt sofort jeden Netzverkehr



## Detaillierte Statistik

- TCP-Verbindungsstatistik
- UDP-Paket-Statistik

Firewall TCP-Verbindungen	
Ankommende zugelassen	16
Ankommende blockiert	0
Abgehende zugelassen	17
Abgehende blockiert	12
Gesamt zugelassen	33
Gesamt blockiert	12

Firewall UDP-Datagramme	
Ankommende zugelassen	216
Ankommende blockiert	4211
Abgehende zugelassen	542
Abgehende blockiert	7
Gesamt zugelassen	758
Gesamt blockiert	4218

Netzwerkverbindungen			
Protokoll	Programmdatei	Remote	Lokal
TCP	ccPxySvc.exe		localhost: 1041
TCP	ccPxySvc.exe	cr1.verisign.com: ...	zam486: 1072
TCP	inetinfo.exe		zam486: 1040
TCP	issCSF.exe		localhost: 1030
TCP	issCSF.exe		localhost: 1032
TCP	issCSF.exe		localhost: 1034

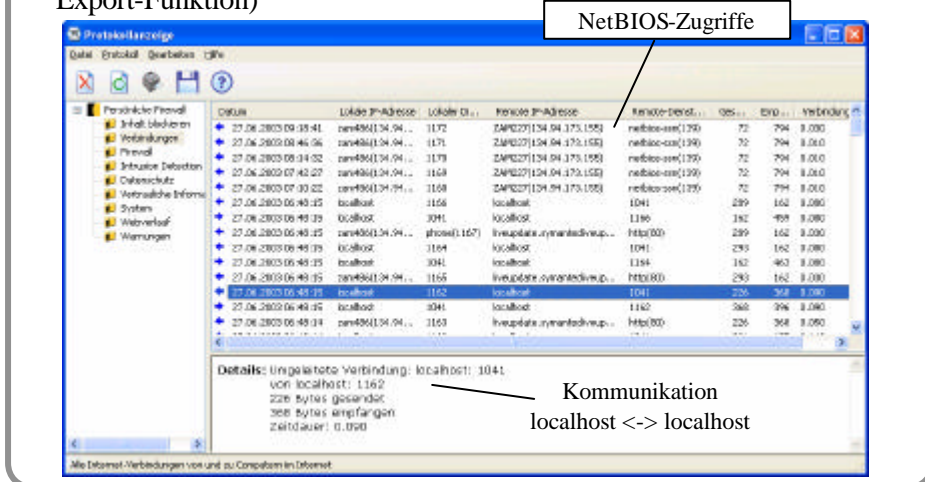
Firewall-Regeln			
Regel	Zugelassen	Blockiert	Weitergegeben
Standard Ankomendes ICMP	3	0	5569
Standard Abgehendes ICMP	3	0	5566
Standard Ankomrender DNS	20	0	5546
Standard Abgehender DNS	11	0	5535
Standard Ankomrender NetBIOS-Name	0	2090	3445
Standard Ankomendes NetBIOS	0	1928	1517
Standard Abgehender NetBIOS	267	0	1250
Standard Ankommende Rückschleifung	85	0	1160
Standard Abgehende Rückschleifung	70	0	1090

- Regelstatistik
- Verbindungsstatistik



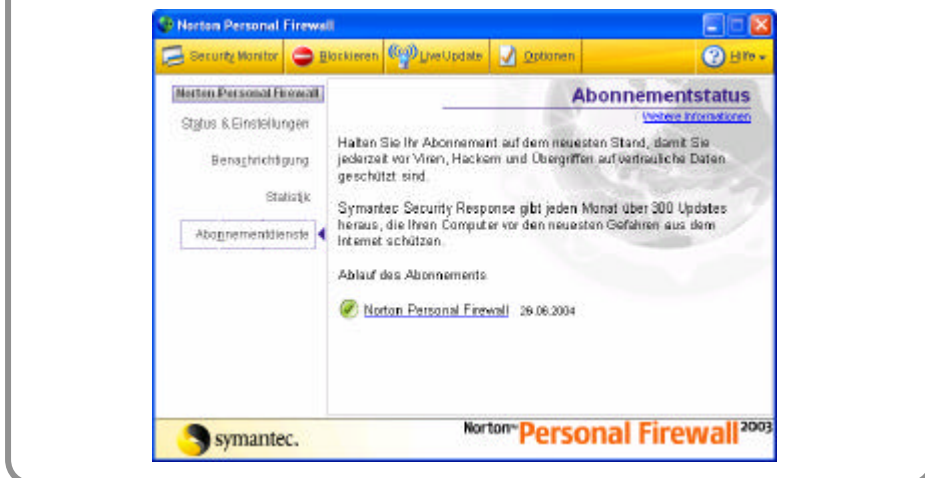
## Protokollanzeige

- Detaillierte Logs aller Verbindungs- und Firewalldaten (mit Druck- und Export-Funktion)



## Abonnementdienste

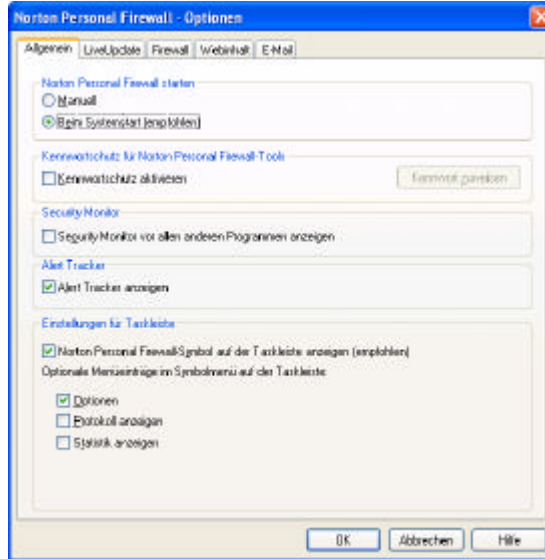
- Zeigt die Laufzeit des Update-Service an (1 Jahr ab Installation)





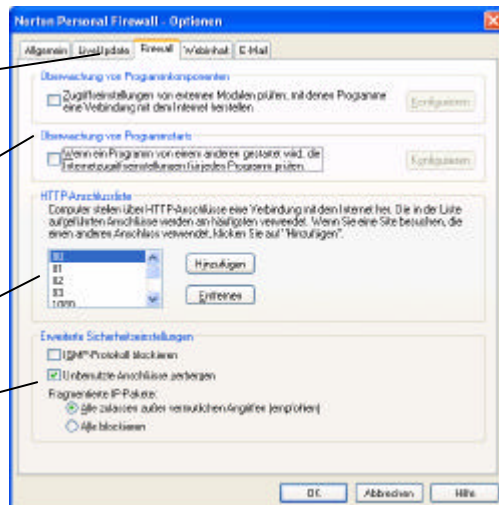
## Menüleiste - Optionen

- Firewall bei Systemstart aktivieren
- Im Produktionsbetrieb ggf. Kennwortschutz aktivieren
- Alert-Tracker anzeigen
- Zugriff auf Konsole über Kontext-Menü des Symbols auf der Taskleiste



## weitere Optionen

- LiveUpdate: Automatisch ausführen und aktualisieren
- Firewall: Zusätzlich zu überwachende Programmkomponenten konfigurieren
- Ports für Webserver hinzufügen
- Unbenutzte IP-Ports verbergen (Stealth-Scan)





# Überwachung von Programmkomponenten

Überwachung von Programmkomponenten	Wenn ein Programm eine externe Softwarekomponente verwendet, um eine Verbindung zum Internet herzustellen, aktivieren Sie Firewall-Regeln für jede Komponente. Auf diese Weise wird sichergestellt, dass sich Trojanische Pferde und andere destruktive Programme nicht an sichere Programme anhängen und so eine Erkennung umgehen können.
Überwachung von Programmstarts	Durch eine Überwachung von Programmstarts können Sie gewährleisten, dass Trojaner und andere destruktive Programme nicht ohne Ihr Wissen sichere Programme starten und manipulieren können. Wenn die Überwachung von Programmstarts aktiviert ist, werden Sie jedes Mal verständigt, wenn ein nicht erkanntes Programm ein anderes Programm startet. Sie können dann entscheiden, ob der Internetzugriff für das unbekannte Programm zugelassen oder blockiert werden soll.



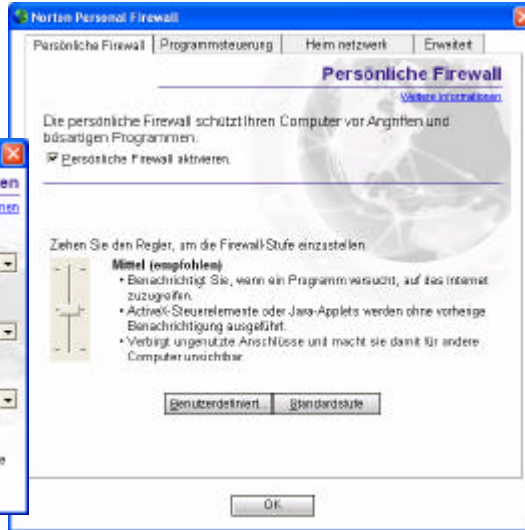
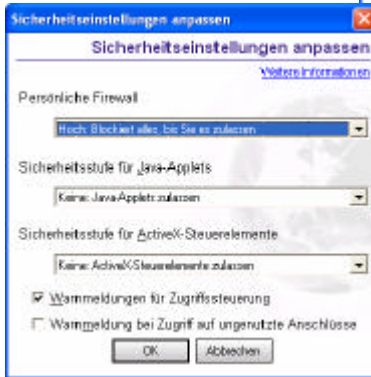
## (aktive) Webinhalte

- Filter können für jede Domain individuell eingestellt werden, etwa für MS-Update



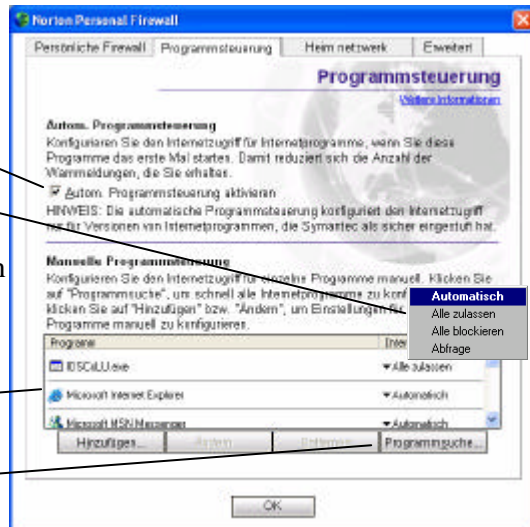
## Persönliche Firewall - Konfigurieren

- Standardeinstellungen für aktive Inhalte (ActiveX, Java)



## Programmsteuerung

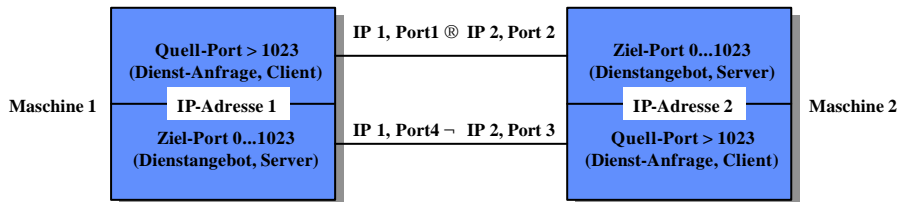
- Automatische Zugriffssteuerung für als sicher bekannte Programme
- Manuelle, individuelle Internet-Zugriffssteuerung für interaktiv bei der ersten Benutzung oder direkt von Hand eingetragene Programme
- Automatische Suche aller Internet-fähigen Programme





## Zur Erinnerung: IP-Kommunikation

- Ein IP-Verbindung zwischen zwei Maschinen wird über "IP-Sockets" mit Hilfe der WinSock-Schnittstelle (WSOCK32(N).DLL) hergestellt:



- Ein Server bietet Dienste im Netz an, indem ein Programm (ein "Dienst") auf einem ganz bestimmten IP-Port (TCP oder UDP) "lauscht"
- Ein Client versucht
  - sich mit diesem Port zu verbinden ("SYNC") und dann über die stehende Verbindung Daten auszutauschen (verbindungsorientiert, TCP)
  - oder einfach Pakete an den Port zu senden und zu hoffen, daß diese ankommen (verbindungslos, UDP)



## Die Funktionsweise des Firewalls

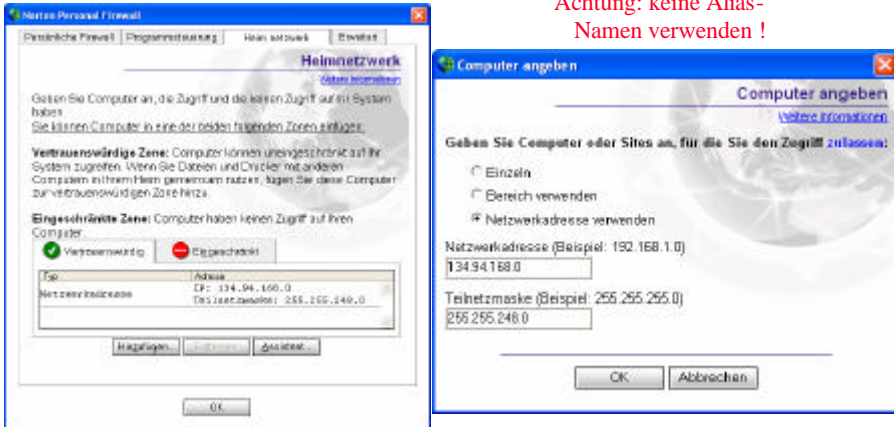
- Für jede einlaufende („Inbound“) oder auslaufende („Outbound“) IP-Verbindungsanforderung oder ICMP-Meldung wird die Liste der als aktiv markierten Regeln **sequentiell von oben nach unten** durchlaufen
- Sobald eine Regel zutrifft („match“), wird ein der Aktionen
  - **Permit:** Verbindung zulassen
  - **Block:** Verbindung nicht zulassen
  - **Ignore:** Verbindung ignorieren, ggf. loggen und Regelliste weiter durchsuchen ausgeführt und das Durchsuchen der Regelliste - außer bei „Ignore“ - abgebrochen
- Wird keine passende Regel gefunden, so wird (falls aktiviert) der **Regelassistent** gestartet
- Eine Verbindung, für die keine gültige Regel gefunden wurde, wird bei nicht aktiviertem Regelassistenten **per Default abgelehnt!**



## Heimnetzwerk (ehem. Internetgruppen)

- Eintrag einzelner Rechner oder Netze für unbeschränkten Zugriff („Vertraut“, z.B. Domain-Server) oder für völliges Zugriffsverbot („Eingeschränkt“)

Achtung: keine Alias-Namen verwenden !



## Erweiterte Firewall-Einstellungen (Regeln)

- Allgemeine Regeln



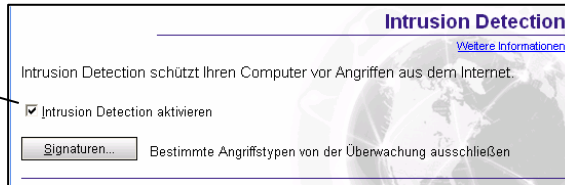
- Und Regeln für Trojaner



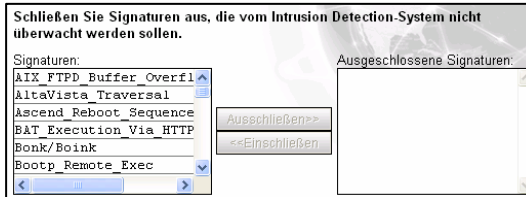
## Intrusion Detection - Konfigurieren

- Intrusion Detection analysiert den einlaufenden Datenverkehr auf bestimmte Muster, die als typisch für Angriffsversuche bekannt sind (und die regelmäßig mit LifeUpdate aktualisiert werden sollten !)

- Aktivieren



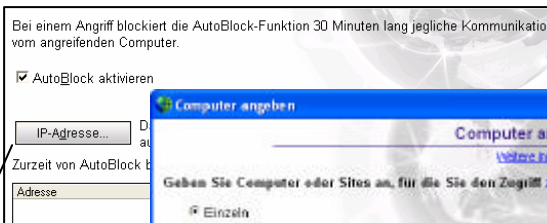
- Auf Wunsch, z.B. für Testzwecke, bestimmte Signaturen aus der Liste entfernen



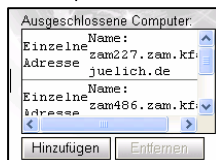
## Autoblock aktivieren

- Automatisches, 30-minütiges Blockieren externer Adressen, die einen Portscan auf dem lokalen PC durchführen (Hacker-Scan)

- Systeme, die legale Scans ausführen, von der Liste der blockierten Systeme ausschließen



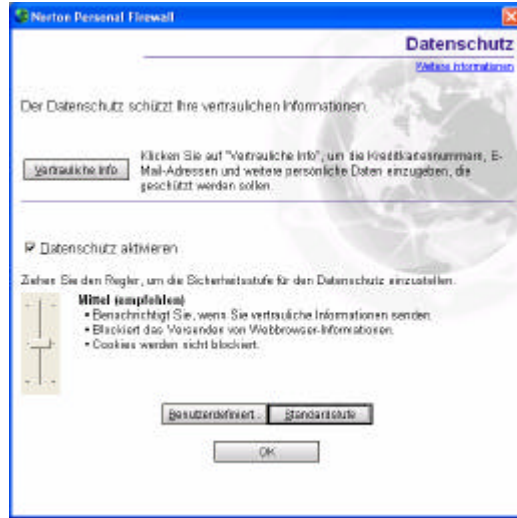
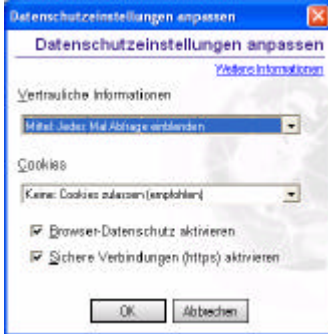
- Dies sind derzeit:  
zam180  
zam227  
zam486





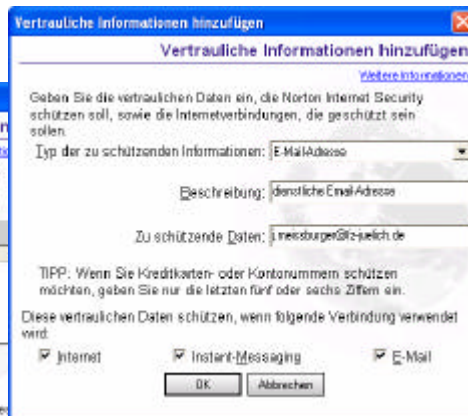
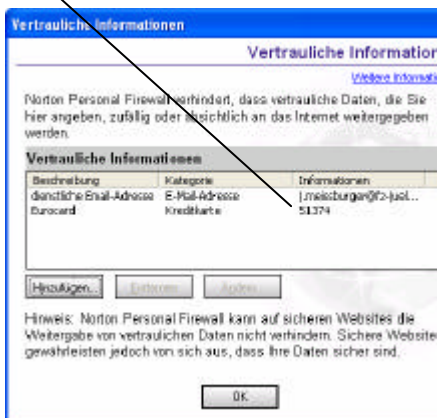
## Datenschutz – Konfigurieren (Webfilter)

- Schutz persönlicher Daten vor versehentlicher Weitergabe in Webformularen und E-Mail
- Tabelle vertraulicher Informationen



## Vertrauliche Informationen eintragen

- Nur Substrings der vertraulichen Information eintragen !



- Jetzt auch für Instant-Messaging und E-Mail !



## Werbeblocker

Der Werbeblocker entfernt unerwünschte Werbebanner und PopUp-Werbung von Webseiten.

- Werbeblocker aktivieren
- Blockieren von PopUp-Fenstern aktivieren

~~Jetzt kaufen und sparen~~ **Papierkorb für Werbung**

**Papierkorb** Mit dem Papierkorb für Werbung können Sie Werbung entfernen und neue Regeln für den Werbeblocker

- und zum Filtern von Werbe-URLs (funktioniert nur beschränkt)



- Zum Verhindern von PopUp-Windows (verhindert manchmal auch die Navigation !)



## Vergleich zu AtGuard

- Unterstützt im Gegensatz zu AtGuard alle Windows-Versionen (+)
- Ein Überblick über alle Firewallregeln ist nur durch Durchsuchen vieler interaktiver Menüs mit Scrolling möglich (für Experten unbequem) (-)
- Der Zugriff von Rechnern und Netzen kann generell über zwei neue Listen „vertraut“ und „eingeschränkt“ geregelt werden (+)
- Der Schutz vor Weitergabe persönlicher Daten (Privacy) wurde durch eine Zeichenketten-basierte Filterfunktion erweitert (+)
- Die Regelerstellung für den Internetzugriff von lokalen Anwendungen auf das Internet (Zugriffssteuerung) kann automatisch erfolgen (+)
- **Norton Personal Firewall bietet auch ohne spezielle Konfiguration einen sehr guten Schutz vor Angriffen aus dem Internet und deren Folgen (++)**



## *Tipps zur Konfiguration*

### **Default-Einstellungen**

### **Kommunikation im Hausnetz**

### **Manuelle Regelerstellung**



## **Grundeinstellungen**

- Die mit der Installation mitgelieferte Default-Einstellung bietet bereits ausreichend Schutz für „normalen“ Kommunikationsbedarf
- Vertrauenswürdige Systeme wie etwa der eigene Domainserver können in die Liste der „vertrauenswürdigen Zone“ eingetragen werden
- Gegebenenfalls kann auch das eigene Hausnetz mit entsprechender Netzmaske komplett in der vertrauenswürdigen Zone eingerichtet werden
- Bei Problemen kann, allerdings *nur testweise*, das gesamte JuNet als vertrauenswertig eingetragen oder aber das Firewall *temporär* völlig abgeschaltet werden. Stets auch das Event-Log überprüfen !
- Vor Softwareinstallationen/Updates Virens Scanner und Firewall am besten abschalten. Wiedereinschalten (Reboot) nicht vergessen !



## Manuelle Regelerstellung

- Startkonfiguration je nach Kommunikationsbedarf auswählen
- Spezielle, immer benötigte Dienste mit „Permit“ zuerst eintragen
- Zeitkritische und häufig benötigte Dienste (Zeitsynchronisation, lokale Kommunikation, DNS-Dienste) an den Listenanfang stellen
- Unerwünschte, spezielle Kommunikationstypen (bestimmte Hosts, bestimmte Dienste) anschließend eintragen
- Allgemeinere, z.B. Netzwerk-weit gültige Regeln zum Schluß eintragen, damit spezifischere Regeln nicht logisch überschrieben werden
- „Benachrichtigung“ zu Beginn auf „Mittel“ oder „Hoch“ einstellen, um den gesamten IP-Verkehr zu beobachten. Event-Log überprüfen !
- Häufige, unerwünschte Dienstanforderungen (meist aus dem Intranet) explizit als spezielle Regel („immer verbieten“) eintragen.



## Der „geschlossene“ PC - localhost

- Netzwerk eingerichtet, aber keinerlei Kommunikation im Netz
- Volle lokale IP-Kommunikation z.B. für die Entwicklung und den Test von Websites (CGI'S, ASP's) oder anderer Client/Server-Anwendungen
- Default-Kommunikation mit localhost = 127.0.0.1
- Default-Kommunikation mit eigener IP-Adresse „myclient“
- Namensauflösung für eigenen Rechner nicht durch Nameserver (BIND), sondern durch lokale Hosts-Datei (oder mit numerischer IP-Adresse):

- Windows NT/2k/XP: C:\%SystemRoot%\system32\drivers\etc\Hosts
- Windows 95/98: C:\%SystemRoot%\Hosts
- mit den Einträgen: 127.0.0.1 localhost  
134.94.xxx.xxx myclient

Pos	Name	Action	Dir.	Protocol	Appl.	Service remote / local	Address remote / local
1	LOCALHOST Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	localhost / Any
2	MYCLIENT Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	myclient / Any



## Individuelle Konfiguration in JuNet

### • Kommunikation mit

- sich selbst, evtl. mit dem eigenen Home-PC im RAS-Netz und mit Rechnern im hausinternen Subnetz (vertrauenswürdige Zone)
- und mit wichtigen Servern im JuNet (domain „kfa-juelich.de“)

134.94.80.2, 134.94.80.3	Nameserver
NTP	Time Server (ntp, time)
DHCP	Dynamic Host Configuration Server
DNS	Distributed Name Service (domain)
WINS	Windows Internet Names Service (nb)
PCSRV	PC-Server des ZAM (nb)
ZELCDS	PC-Server des ZEL (nb)
IMAPSRV.fz-juelich.de	Mailserver (imap, imap-ssl)
POPSRV.fz-juelich.de	Mailserver (pop3)
MAILRELAY.fz-juelich.de	Mailgateway (smtp)
HTTP, HTTPS	WWW-Server des FZJ
BACKUPSRV	Tivoli-Backupserver
134.94.117.0	RAS-Netz (Netzmaske 255.255.255.0)